

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH APPLE
ID MAXX3644@ICLOUD.COM THAT IS
STORED AT PREMISES CONTROLLED BY
APPLE, INC.

Case No. 3:20-mj-33

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jacob R Guffey, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an Application for a Search Warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I have been a Special Agent since 2008 and I am currently assigned to the Charlotte Division, Hickory Resident Agency. In this capacity, I am assigned to investigate cases involving Child Pornography, corporate fraud, public corruption, and similar violations. From 2012 to 2015, I worked on the Navajo Indian Reservation, located within the Area of Responsibility of the Albuquerque Division, Gallup Resident Agency. At that assignment I conducted and participated in numerous death investigations, child sexual assaults, and other federal crimes occurring within the boundaries of Indian Country. From 2008 to 2012 I investigated Health Care Fraud in the

Miami Division. I have personally been the case agent for numerous investigations that have resulted in the indictment and conviction of numerous subjects. I have also participated in ordinary methods of investigation, including but not limited to, consensual monitoring, physical surveillance, interviews of witnesses and subjects, and the use of confidential informants. I am an active member of the Evidence Response Team. Accordingly, I have executed numerous search warrants and seized evidence. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show simply that there is sufficient probable cause for the requested Search Warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this Affidavit, there is probable cause to believe that the information described in Attachment A contains evidence and contraband (in the form of child pornography) of violations of 18 U.S.C. § 2252A Sexual exploitation of children, as described in Attachment B.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. § 2252A relating to materials involving the sexual exploitation of minors.

- a. 18 U.S.C. § 2252A(a)(1) makes it a crime to knowingly transport or ship, using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer, any visual depiction if the

producing of such visual depiction involving the use of a minor engaging in sexually explicit conduct and such visual depiction was of such conduct.

- b. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, by any means including by computer, or any material that contains child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer
- c. 18 U.S.C. § 2252A(a)(5)(B) prohibits knowingly possessing or knowingly accessing with intent to view any book, magazine, periodical, film, video tape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

JURISDICTION

6. This Court has jurisdiction to issue the requested Search Warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:
- a. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
 - b. “Child Pornography” includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).
 - c. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” *See* 18 U.S.C. § 1030(e)(1).
 - d. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output

devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- e. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- f. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- g. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- h. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. Like a phone number, no two computers or network of computers connected to the internet are assigned the same IP address at exactly the same date and time. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.
- i. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).
- j. “Sexually explicit conduct” refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).
- k. “Shared Folder” is a folder of files stored on a computer’s local hard disk drive that can be used (or shared) by other users on the network or internet.
- l. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).
- m. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives,

videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

PROBABLE CAUSE

8. The Federal Bureau of Investigation is investigating the transportation and possession of child pornography by Larry Haynes (Haynes), date of birth February 12, 1956, a resident of Catawba County, North Carolina which is within the boundaries of the Western District of North Carolina. The information was received through the submission of a cyber-tip from Apple to the National Center for Missing and Exploited Children (NCMEC).

9. The details set forth in this affidavit show that there is probable cause that Haynes attempted to send child pornography from one of his email addresses, maxx3644@icloud.com, to another one of his email addresses, mwell689@yahoo.com.

10. On or about May 17, 2019, Apple submitted cyber tip 49666753 to NCMEC.

11. In the cyber tip Apple provided four emails, with attached images, sent from an Apple account created by Haynes; email address maxx3644@icloud.com. NCMEC advised the

Affiant that Apple had viewed the emails and attached images. The following details were provided for the emails:

- a. Sent on May 15, 2019, at 08:31:49 -0400
 - i. From: Lars <maxx3644@icloud.com>
 - ii. To: mwell689@yahoo.com
 - iii. Subject: E
- b. Sent on May 15, 2019, at 08:36:39 -0400
 - i. From: Lars maxx3644@icloud.com
 - ii. To: mwell689@yahoo.com
 - iii. Subject: Re
- c. Sent on May 15, 2019, at 08:37:48 -0400
 - i. From: Lars maxx3644@icloud.com
 - ii. To: mwell689@yahoo.com
 - iii. Subject: 1
- d. Sent on May 15, 2019, at 08:38:03 -0400
 - i. From: Lars maxx3644@icloud.com
 - ii. To: mwell689@yahoo.com

iii. Subject: 2

12. On July 18, 2019, Apple responded to a subpoena sent by the FBI. Apple provided information regarding additional emails associated with Haynes' Apple account. One of the verified email addresses on Haynes' Apple account was the recipient of the aforementioned emails, mwell689@yahoo.com.

13. In addition to the emails, Apple provided NCMEC with four viewable images depicting child pornography which were associated with an Apple account created by Haynes; email address: maxx3644@icloud.com; ESP User ID: 1664712388. A summary of the images is as follows:

- a. Image named, "IMG_1952.JPG", is of a nude female who appears under the age of 10. She is squatted down, leaning back on her hands with her legs apart. Her vagina is the focal point of the image.
- b. Image named, "IMG_1953.JPG", is of a nude female who appears to be under the age of 16. She is sitting on the floor with her legs apart. Her vagina is the focal point of the image.
- c. Image named, "IMG_1954.JPG", is of a female who appears to be under the age of 12. She is nude from her waist down. She has her leg propped up. Her vagina is the focal point of the image.
- d. Image named, "IMG_1955.JPG", is of a female who appears to be under the age of 12. She is nude from her waist down. She has a leg lifted in the air. Her vagina is the focal point of the image.

14. Apple also provided NCMEC an email content report. The report was not reviewed by Apple prior to submission to NCMEC. That information was provided to your Affiant on a CD. Your Affiant has not reviewed the email content report material.

15. On June 26, 2019, and based on the information provided in the cyber tip, investigators submitted subpoena number 535434 to Apple requesting information that would help identify a subject associated with the Apple account.

16. On July 18, 2019, Apple provided the following information pertaining to Haynes;
Email Address: maxx3644@icloud.com; ESP User ID: 1664712388:

- a. Apple ID: maxx3644@icloud.com
- b. DS ID: 1664712388
- c. Account Type: Full iCloud
- d. First Name: Larry
- e. Last Name: Haynes
- f. Country: US (United States)
- g. Language: US-EN
- h. Time Zone: US/Pacific
- i. Account Status: Active
- j. Created On: Tues, 08 Jan 13 15:29PT

- k. Address Line 1: 4097 Mt Beulah Rd
- l. City: Maiden, North Carolina
- m. Country Code: United States
- n. Day Phone 1-704-779-1295
- o. Registration IP Address: 184.39.11.3
- p. Additional Emails:
 - i. maxx3644@icloud.com – primary, verified
 - ii. maxx3644@icloud.com – additional verified
 - iii. mwell689@yahoo.com – additional verified
- q. Game Center Nickname: ca7vflrg74ljp

17. On September 5, 2019, an administrative subpoena was served to AT&T to provide information regarding iTunes Transaction IP address: 99.111.132.129 from May 15, 2019, 15:53:54 GMT. This information was previously provided by Apple.

18. On September 10, 2019, AT&T replied with the following Customer information:
- a. Name: Jeannette Haynes
 - b. Account number: 143015331
 - c. Status: A

- d. Address 1: 4097 Mount Beulah Rd, Maiden, NC, 28650-9423
- e. Address 2: Jeannette Haynes 4097 Mount Beulah Rd, Maiden, NC, 2865-9423
- f. Email: spogetti@yahoo.com
- g. Phone: 704-483-0549
- h. IP Address Start Date: May 14, 2019, 11:06am
- i. IP Address End Date: June 4, 2019, 07:38am

19. Your Affiant is aware that Jannette Haynes lives at the same residence as Larry Haynes and is possibly his spouse.

- a. Listed as a First Degree Relative, with an age of 60, in public record searches. (Larry Haynes is approximately 63 years old)
- b. Listed on property deed as Grantor with Larry Haynes for 4097 Mount Beulah Rd, Maiden, NC, 2865-9423.

20. On August 12, 2019, investigators sent a preservation request to Apple requesting the preservation of any and all records related to Haynes; email address: maxx3644@icloud.com; ESP User Identifier: 1664712388; CyberTip Report: 4966675. The request was valid for 90 days.

21. On November 1, 2019, investigators sent a second preservation request to Apple requesting an extension of the previous preservation request for an additional 90 days.

22. On November 14, 2019, your Affiant spoke with a representative at Apple who was familiar with the aforementioned cyber tip. Your Affiant learned that Apple recognized the email

attachments as known child pornography by screening attachments against known child pornography, prior to the email being sent. The emails sent by maxx3644@icloud.com were four (4) attempts to send the same email to mwell689@yahoo.com. The emails were stopped from leaving Apple and a cyber tip was created. Apple opined that the user was sending the images to a different email account, albeit his own account, thus creating cloud storage. Apple did not know where the images were attached from. Apple knew an iPad was used in the attempt to send the emails.

23. On November 15, 2019, your Affiant served a preservation letter to Yahoo via Oath Holdings, through their online portal, for email address mwell689@yahoo.com.

24. On November 25, 2019, your Affiant served a subpoena to Yahoo, Inc, via Oath Holdings requesting subscriber information for email address mwell689@yahoo.com with specified date range for activity during May 14, 2019 through May 16, 2019.

25. On November 26, 2019, your Affiant received the following information in response to that subpoena:

- a. Account Status: Active
- b. Registration IP Address: 74.235.49.88
- c. Created: December 20, 2013 16:41:15 UTC
- d. Full Name: Larry Haynes
- e. Verified telephone number: 1-704-779-1296
- f. Login information for User ID mwell689:

- i. IP Address: 2600:1702:26a0:1510:94ab:c44f:1327:df6b, May 16, 2019
19:34:27 UTC
- ii. IP Address: 2600:1702:26a0:1510:94ab:c44f:1327:df6b, May 16, 2019
19:34:27 UTC
- iii. IP Address: 2600:1702:26a0:1510:4c45:f380:193:bdbf, May 15, 2019
23:16:34 UTC

26. On November 29, 2019, your Affiant conducted an open source search and learned that the IP Addresses provided by Oath Holdings were associated with internet provider AT&T.

27. On November 29, 2019, your Affiant submitted a subpoena to AT&T requesting subscriber information for the dates and times and IP Addresses provided by Oath Holdings.

28. On December 1, 2019, AT&T provided the following information in response to the subpoena:

- a. Activation time stamp: October 31, 2017, 17:22:48 GMT
- b. Attftxipv6iapd: 2600:1702:26a0:1510::/60
- c. IP Address Assigned: 99.111.132.129
- d. User ID: jeannettehaynes@att.net
- e. Site ID: 111974834
- f. Contact name: Jeannette Haynes
- g. MAC Address: dc:7f:a4:a6:bf:58

- h. Account ID: 143015331
- i. Primary Contact Information:
 - i. Contact Name: Jeanette Haynes
 - ii. Preferred email: mwell689@yahoo.com
 - iii. Account established: March 11, 2015
- j. Service Address 4097 Mt Beulah Rd, Maiden, NC, 28650

29. In summary, upon receipt of this cyber tip you're your Affiant and other investigators determined the email addresses used to send and potentially receive child pornography belonged to Larry Haynes. It was determined Jeannette Haynes was the subscriber for the internet service from where Larry Haynes attempted to send the emails and child pornography. It was also determined that Larry Haynes and Jeannette Haynes live at the same residence and are likely married. Your Affiant is seeking a search warrant to obtain information from the address from which the email was sent. That information is specified in Attachment B.

30. Based on my training and experience and the training and experience of others with whom I have worked, there is probable cause to believe content stored on behalf and information associated with Apple ID maxx3644@icloud.com contain relevant and material information the ongoing criminal investigation, including but not limited to 1) picture and or video files of underage females either engaging in sexual acts or naked and displayed in a lewd and lascivious manner; 2) messages or documentation specifying Haynes's location(s); 3) IP address login information that may be helpful in identifying Haynes's location(s) at various dates and times and

4) information that may reveal other relevant electronic communication accounts associated with the possession and transport of child pornography.

INFORMATION REGARDING APPLE ID AND iCloud¹

31. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

32. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

33. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

34. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

35. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated

with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

36. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

37. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an

Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

38. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

39. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where,

and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

40. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

41. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

42. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan

to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

43. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

44. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

45. I anticipate executing this Search Warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the Search Warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

46. Based on the forgoing, I believe there is probable cause that fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 2252 relating to materials involving the sexual exploitation of minors may be associated with Apple ID maxx3644@icloud.com, and be in the possession of Apple. I therefore request that the Court issue the proposed Search Warrant.

47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this Search Warrant.

48. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, Apple shall disclose responsive data by sending it to: FBI Special Agent Jacob R Guffey, 231 Government Ave SW, Suite 303, Hickory, NC, 28602; or via email to jrguffey@fbi.gov.

REQUEST FOR SEALING

49. I further request that the Court order that all papers in support of this Application, including the Affidavit and Search Warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.


REQUEST FOR NON-DISCLOSURE

50. I further request that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), Apple be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this Search Warrant until further order of the Court. Such an order is justified because notification of the existence of this Search Warrant would

seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.

WHEREFORE, it is respectfully requested that the Court grant the attached Order directing Apple not to disclose the existence of the Search Warrant or the Application except to the extent necessary to carry out the Order.

Respectfully submitted,



Jacob R Guffey
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on JANUARY 28, 2020__



HONORABLE DAVID KEESLER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This Search Warrant applies to information associated with maxx3644@icloud.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents (and content logs) of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files). The Provider is hereby ordered to disclose the above information to the government within up to 14 days of service of this Search Warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 2252A, Sexual exploitation of children involving Larry Haynes, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Evidence of violations relating to 18 U.S.C. § 2252A as described in Paragraphs 8-27 of the Affidavit.
- b. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- c. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- d. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- e. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to

locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ (pages/CDs/megabytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature